CH 678134 A5

(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
BUNDESAMT FÜR GEISTIGES EIGENTUM

(11) CH 678134 A5

(51) Int. Cl.[5]: H 04 K 1/02
H 04 L 9/28

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT A5

(21) Gesuchsnummer: 105/89

(22) Anmeldungsdatum: 13.01.1989

(24) Patent erteilt: 31.07.1991

(45) Patentschrift veröffentlicht: 31.07.1991

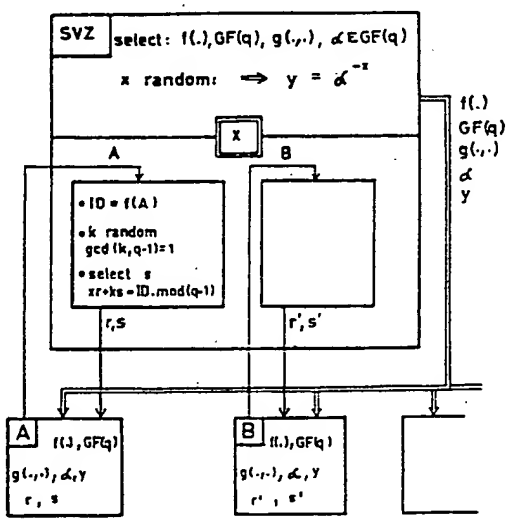
(73) Inhaber:
Ascom Radiocom AG, Solothurn

(72) Erfinder:
Günther, Christoph, Dr., Fislisbach

(74) Vertreter:
ASEA Brown Boveri AG, Baden

(54) Verfahren zum authentifizierten Schlüsselaustausch.

(57) Der erfindungsgemässe Schlüsselaustausch findet in einem Netz mit einer Schlüsselverteilzentrale SVZ und mehreren Benutzern A, B, ... statt und weist zwei Phasen auf, nämlich eine Präauthentifikationsphase und eine Schlüsselaustauschphase. In der Präauthentifikationsphase kommt jeder Benutzer A, B, ... zur Schlüsselverteilzentrale SVZ und lässt sich seine Identität mit dem ElGamal Schema signieren. In der nachfolgenden Schlüsselaustauschphase erzeugen zwei Benutzer A und B einen gemeinsamen Geheimschlüssel z nach einem abgeänderten Diffie-Hellmann Verfahren.



Beschreibung

Technisches Gebiet

Die Erfindung betrifft ein Verfahren zum authentifizierten Schlüsselaustausch in einem Netz mit einer Schlüsselverteilzentrale und mehreren Teilnehmern.

Stand der Technik

Verfahren zur Erzeugung von authentifizierten Geheimschlüsseln werden z.B. in der europäischen Patentanmeldung EP-A 0 307 627 und in der deutschen Auslegeschrift DE-A 3 915 262 beschrieben.

Das erste der beiden Verfahren führt die Authentifikation über das öffentliche Telefonnetz durch und ist entsprechend nicht für alle Anwendungen gleichermassen geeignet. Das zweite Verfahren verwendet eine präauthentifizierte Liste von öffentlichen Teilnehmerschlüsseln und ist für den automatischen Betrieb entworfen worden. Bei der Aufnahme einer Verbindung muss jedoch der öffentliche Teilnehmerschlüssel jeweils aus der präauthentifizierten Liste gelesen werden. Dabei gibt es zwei Möglichkeiten: Entweder wird die Liste in jedem Gerät gespeichert, was bei grossen Netzen viel Speicherplatz (proportional zur Teilnehmerzahl) beansprucht und bei Netzerweiterungen eine aufwendige Informationsübertragung verlangt, oder die Liste wird zentral geführt, was bei jedem Verbindungsaufbau zwei Rückfragen an die Schlüsselverteilzentrale verlangt.

Eine zentrale Liste mit lokalen Auszügen stellt für viele Anwendungen eine vernünftige Lösung dar. Dort wo jedoch die Verbindung bei wenig Speicherplatz, autonom aufgebaut werden soll und eine Authentifikation der Teilnehmer einzeln notwendig ist, ist auch dieses Verfahren nicht sehr hilfreich. Beispiele dafür sind Netze von POS-Terminals, mobile Telefonsysteme und sonstige Funknetze sowie Computernetze.

Zur Identifikation (u.a. an POS-Terminals) sind von

– Fiat und Shamir («How to Prove Yourself: Practical Solutions to Identification and Signature Problems», Advances in Cryptology – CRYPTO'86, Lecture Notes in Computer Science, Vol 263, pp. 186–194, Springer Verlag 1987),

– L.C. Guillou, J.-J. Quisquater («A Practical Zero Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory, Advances in Cryptology – EUROCRYPT'88, Lecture Notes in Computer Science, Vol 330, pp. 123–128, Springer Verlag 1988), und von

– T. Beth, («Efficient Zero Knowledge Identification Scheme for Smart Cards», Advances in Cryptology – EUROCRYPT'88, Lecture Notes in Computer Science, Vol. 330, pp. 77–84 Springer Verlag 1988) sogenannte «zero knowledge proofs» vorgeschlagen worden. Bei einem solchen «zero knowledge proof» geht jeder Benutzer in einer Präauthentifikationsphase zur Schlüsselverteilzentrale, weist sich aus und bekommt von der Zentrale den öffentlichen Netzschlüssel sowie die zu seiner Identität ID (z.B. AHV-Nummer) gehörige Signatur S (ID), welche die Zentrale mit dem geheimen Netzschlüssel bildet.

Will sich nun A gegenüber einem anderen Benutzer B ausweisen, so beweist er in einem Protokoll mit B, dass er S(ID) kennt, ohne die Signatur selbst preiszugeben. Die Signatur wird dabei unter Verwendung des öffentlichen Netzschlüssels geprüft.

Darstellung der Erfindung

Aufgabe der Erfindung ist es, ein Verfahren zum authentifizierten Schlüsselaustausch in einem Netz mit einer Schlüsselverteilzentrale und mehreren Teilnehmern anzugeben, welches flexibel in bezug auf die Erweiterung durch neue Benutzer ist, einen geringen Speicherbedarf hat und die Nachteile der bekannten Verfahren vermeidet.

Erfindungsgemäss besteht die Lösung darin, dass in einer Präauthentifikationsphase

a) die Schlüsselverteilzentrale eine Funktion f(.) zur Erzeugung von Identitätsnummern, einen endlichen Körper GF(q), in welchem die Rechenoperationen ausgeführt werden, eine Funktion g: GF(q) x GF(q) → GF(q), ein primitives Element $\alpha \in GF(q)$ und eine geheime erste Zufallszahl x wählt, aus welchen sie einen öffentlichen Netzschlüssel $y = \alpha^{-x}$ bildet,

b) die Schlüsselverteilzentrale jedem Benutzer eine Identitätsnummer ID = f(A) signiert, indem die Schlüsselverteilzentrale eine geheime zweite Zufallszahl k wählt, welche die Eigenschaft gcd(k,q–1) = 1 hat, aus der Zufallszahl k einen öffentlichen Benutzerschlüssel $r = \alpha^k$ und einen geheimen Benutzerschlüssel s mit der Eigenschaft xr+ks = ID mod (q–1) bildet und dem Benutzer seine beiden Benutzerschlüssel mitteilt,

und dass in einer Schlüsselaustauschphase zwischen einem ersten Benutzer A und einem zweiten Benutzer B

c) jeder der beiden Benutzer A resp. B dem anderen seinen öffentlichen Benutzerschlüssel r resp. r' mitteilt,

d) jeder der beiden Benutzer A resp. B die Identitätsnummer ID' = f(B) resp. ID = f(A) bildet und aus dieser Identitätsnummer und dem Benutzerschlüssel r' resp. r des jeweils anderen eine Grösse $r's' = \alpha^{ID'}y^{r'}$ resp. $r^s = \alpha^{ID}y^r$ bildet,

e) jeder der beiden Benutzer A resp. B eine geheime Zufallszahl t resp. t' erzeugt und damit einen Code r^t resp. $r^{t'}$ bildet, welchen er dem anderen Benutzer B resp. A mitteilt und

f) die beiden Benutzer A und B einen gemeinsamen geheimen Kommunikationsschlüssel

$z = g(r^{t's}, r^{s't})$ bilden.

Es versteht sich von selbst, dass der endliche Körper GF(q) so gewählt wird, dass q–1 eine Zahl mit mindestens einem grossen Primfaktor ist. Bis auf eine werden alle erfindungsgemässen Operationen in diesem Körper ausgeführt.

Mit den bekannten «zero knowledge proof» Verfahren hat die Erfindung die Eigenschaft gemeinsam, ebenfalls die Signatur der Identität S(ID) als

geheimes Authentifikationsmerkmal zu benutzen. Im Unterschied zu den bekannten Verfahren wird dieses Merkmal jedoch zur Konstruktion eines gemeinsamen, gegenseitig authentifizierten Schlüssels verwendet.

Aus den abhängigen Patentansprüchen ergeben sich vorteilhafte Ausführungsformen der Erfindung.

Kurze Beschreibung der Zeichnung

Nachfolgend soll die Erfindung anhand von Ausführungsbeispielen im Zusammenhang mit der Zeichnung näher erläutert werden. Es zeigen:

Fig. 1 eine schematische Darstellung der Präauthentifikationsphase; und

Fig. 2 eine schematische Darstellung der Schlüsselaustauschphase zwischen zwei Benutzern.

Die in der Zeichnung verwendeten Bezugszeichen und deren Bedeutung sind in der Bezeichnungsliste zusammenfassend tabelliert.

Wege zur Ausführung der Erfindung

Der erfindungsgemässe Schlüsselaustausch findet in einem für die Übertragung von digitalen Daten geeigneten Netz mit einer Schlüsselverteilzentrale SVZ und mehreren Benutzern A, B,... statt und weist zwei Phasen auf, nämlich eine Präauthentifikationsphase und eine Schlüsselaustauschphase. In der Präauthentifikationsphase kommt jeder Benutzer A, B,... zur Schlüsselverteilzentrale SVZ und lässt sich seine Identität gemäss dem El-Gamal-Schema signieren. In der nachfolgenden Schlüsselaustauschphase erzeugen zwei Benutzer A und B einen gemeinsamen Geheimschlüssel z nach einem abgeänderten Diffie-Hellmann-Verfahren.

Fig. 1 zeigt eine schematische Darstellung der Präauthentifikationsphase. Als erstes wählt (SELECT) die Schlüsselverteilzentrale SVZ einen endlichen Körper GF(q), wobei q–1 typischerweise einen grossen Primfaktoren aufweist, und ein primitives Element $\alpha \in GF(q)$. Dann erzeugt sie zufällig (RANDOM) als geheimen Netzschlüssel («private part») eine erste Zahl x, aus welcher sie einen öffentlichen Netzschlüssel (»public part») $y = \alpha^{-x}$ bildet. (Es versteht sich, dass diese und die später beschriebenen Operationen im endlichen Körper GF(q) ausgeführt werden, wenn es nicht explizit anders spezifiziert wird.) Weiter definiert sie eine geeignete Funktion f(.), welche aus den Identitätsmerkmalen eine eindeutige Identitätsnummer erzeugt. Schliesslich definiert sie noch eine geeignete Funktion g: $GF(q) \times GF(q) \rightarrow GF(q)$. Vorzugsweise ist diese Funktion das Produkt.

Die durch f(.) bestimmte Identitätsnummer ID kann beispielsweise durch Abtasten des Fingers (Fingerabdruck) gebildet werden. Es können aber auch weitere Merkmale eingehen. Typischerweise ist f(.) eine Einwegfunktion (one way function), die auf den Datenstring bestehend aus Namen, Vornamen, Geburtsdatum und eventuell weiteren Merkmalen angewandt wird.

Den endlichen Körper GF(q), das primitive Element α und den öffentlichen Netzschlüssel y sowie die Funktion f(.) gibt die Schlüsselverteilzentrale SVZ öffentlich bekannt. Den geheimen Netzschlüssel x speichert sie zugriffsgeschützt ab.

Die Schlüsselverteilzentrale SVZ hat damit die grundlegenden, allgemeinen Vorbereitungen abgeschlossen. Nun kommt jeder Benutzer zur Schlüsselverteilzentrale SVZ und lässt sich seine Identität gemäss dem El-Gamal-Schema signieren.

Der Benutzer A weist sich aus (z.B. mit seinem Reisepass), worauf die Schlüsselverteilzentrale SVZ mit Hilfe der Funktion f(.) eine eindeutige Identitätsnummer $ID = f(A)$ berechnet. Dann erzeugt sie zufällig (RANDOM) eine benutzerspezifische Zahl k, welche die Eigenschaft $gcd(k,q-1) = 1$ hat (gcd = greatest common divisor). Aus der zweiten Zufallszahl k bildet sie einen öffentlichen Benutzerschlüssel $r = \alpha^k$ und einen geheimen Benutzerschlüssel s mit der Eigenschaft $xr+ks = ID \bmod (q-1)$. Die beiden Benutzerschlüssel r und s teilt sie dem Benutzer A mit, der den geheimen Benutzerschlüssel s zugriffsgesichert abspeichert.

Jeder Benutzer, der im Netz zugelassen werden will, muss die beschriebene Präauthentifikationsphase durchlaufen.

Fig. 2 zeigt eine schematische Darstellung der Schlüsselaustauschphase. Sie findet zu Beginn einer Kommunikation zwischen einem ersten Benutzer A und einem zweiten Benutzer B statt.

Jeder der beiden Benutzer kennt dabei die öffentlich bekannten Parameter f(.), g(.,.), GF(q), α, y, sowie seine Schlüssel r und s resp. r' und s'. Typischerweise hat er auch seine eigene Identitätsnummer ID resp. ID' abgespeichert.

Die beiden Benutzer A und B berechnen als erstes die Identitätsnummer ID' und ID und tauschen den öffentlichen Benutzerschlüssel r und r' aus.

Als zweites bildet jeder der beiden Benutzer A resp. B aus der Identitätsnummer ID' resp. ID und dem Benutzerschlüssel r' resp. r des jeweils anderen eine Grösse $r^{s'} = \alpha^{ID'y^{r'}}$ resp. $r^s = \alpha^{IDy^r}$. Als drittes erzeugen sie zufällig (RANDOM) je eine geheime Zahl t resp. t' und errechnen daraus je einen Code r^t resp. $r^{t'}$. Dann wird dieser Code r^t resp. $r^{t'}$ ausgetauscht. Zum Schluss bildet jeder der beiden Benutzer A resp. B aus den bekannten Grössen den gemeinsamen Geheimschlüssel («session key»)

$z = g(r^{t's}, r^{s't})$.

Das erfindungsgemässe Verfahren hat u.a. folgende Vorteile:

1. Ausser den eigenen Identifikationsmerkmalen genügt die Kenntnis eines einzigen «public keys» zum authentifizierten Schlüsselaustausch mit einem beliebigen anderen Benutzer des Netzes. Das Verfahren zeichnet sich folglich durch einen sehr geringen Speicherbedarf aus.

2. Jeder präauthentifizierte Benutzer kann mit jedem anderen präauthentifizierten Benutzer einen authentifizierten Schlüsselaustausch vornehmen, ohne dabei auf die Schlüsselverteilzentrale zurückgreifen zu müssen (off-line authentifizierter

Schlüsselaustausch). Ein mit diesem System betriebenes Netz ist dadurch auch beliebig flexibel in bezug auf Erweiterung des Teilnehmerkreises.

3. Dennoch sind bei dem erfindungsgemässen Schlüsselaustausch alle Teilnehmer unterscheidbar, d.h. es kann sich keiner für einen anderen ausgeben.

Zur Sicherheit des erfindungsgemässen Schlüsselaustausches lässt sich folgendes sagen:

1. Falls man s aus α, y, ID und r bestimmen kann, kann man das El-Gamal'sche Signaturschema brechen, welches allgemein als sicher angesehen wird.

2. Falls man $(r^{r'})^s$ aus r, r^s und $r^{r'}$ bestimmen kann, kann man den Diffie-Hellmann'schen Schlüsselaustausch-Algorithmus brechen, welcher ebenfalls allgemein als sicher angesehen wird.

Diese Überlegungen lassen es als wahrscheinlich erscheinen, dass bei geeigneter Wahl von q, α, x und k die Kenntnis von s resp. s' durch den Benutzer A resp. B unerlässlich ist für die Konstruktion des Sitzungsschlüssels z. Das erfindungsgemässe Schlüsselaustauschverfahren beinhaltet somit eine gegenseitige Authentifikation der Benutzer A und B.

Der resultierende Sitzungsschlüssel z kann nun für die verschiedensten Anwendungen benutzt werden, wie z.B. zur Chiffrierung, zur Sicherung der Datenintegrität oder auch nur zur Identitätskontrolle.

Das erfindungsgemässe Verfahren lässt sich mit als solchen bekannten Mitteln realisieren. Eine für den authentifizierten Schlüsselaustausch zwecks Chiffrierung geeignete Anordnung ist z.B. in der eingangs erwähnten deutschen Auslegeschrift DE-A 3 915 262 beschrieben.

Die Einsatzmöglichkeiten des beschriebenen Verfahrens sind aufgrund der erwähnten Vorteile ziemlich breit: Mobiles Telephon, Militärfunk, Computernetze und POS-Terminals.

Das beschriebene Schlüsselaustauschverfahren ist ein «public key» Verfahren mit einem einzigen Schlüssel, das einen authentifizierten Schlüsselaufbau zwischen zwei beliebigen Benutzern erlaubt. Es wird off-line betrieben, ist flexibel in bezug auf Erweiterungen durch neue Benutzer und hat einen geringen Speicherbedarf. Der Rechenaufwand ist im wesentlichen der gleiche wie beim weit verbreiteten Diffie-Hellmann-Verfahren. Die etwas aufwendigere El-Gamal Signatur wird jeweils von der Schlüsselverteilzentrale und ausserdem für jeden Benutzer nur einmal durchgeführt.

Patentansprüche

1. Verfahren zum authentifizierten Schlüsselaustausch in einem Netz mit einer Schlüsselverteilzentrale und mehreren Teilnehmern A, B, dadurch gekennzeichnet, dass in einer Präauthentifikationsphase

a) die Schlüsselverteilzentrale eine Funktion f(.) zur Erzeugung von Identitätsnummern, einen endlichen Körper GF(q), in welchem die Rechenoperationen ausgeführt werden, eine Funktion g: GF(q) x GF(q) $\rightarrow$ GF(q), ein primitives Element $\alpha \in$ GF(q) und eine geheime erste Zufallszahl x wählt, aus welchen sie einen öffentlichen Netzschlüssel $y = \alpha^{-x}$ bildet,

b) die Schlüsselverteilzentrale jedem Benutzer eine Identitätsnummer ID = f(A) signiert, indem die Schlüsselverteilzentrale eine geheime zweite Zufallszahl k wählt, welche die Eigenschaft gcd(k, q–1) = 1 hat, aus der Zufallszahl k einen öffentlichen Benutzerschlüssel $r = \alpha^k$ und einen geheimen Benutzerschlüssel s mit der Eigenschaft $xr+ks \equiv ID \bmod (q-1)$ bildet und dem Benutzer seine beiden Benutzerschlüssel mitteilt,

und dass in einer Schlüsselaustauschphase zwischen einem ersten Benutzer A und einem zweiten Benutzer B

c) jeder der beiden Benutzer A resp. B dem anderen seinen öffentlichen Benutzerschlüssel r resp. r' mitteilt,

d) jeder der beiden Benutzer A resp. B die Identitätsnummer ID' = f(B) resp. ID = f(A) bildet und aus dieser Identitätsnummer und dem Benutzerschlüssel r' resp. r des jeweils anderen eine Grösse $r'^{s'} = \alpha^{ID'}y^{r'}$ resp. $r^s = \alpha^{ID}y^r$ bildet,

e) jeder der beiden Benutzer A resp. B eine geheime Zufallszahl t resp. t' erzeugt und damit einen Code r^t resp. r'^t bildet, welchen er dem anderen Benutzer B resp. A mitteilt und

f) die beiden Benutzer A und B einen gemeinsamen geheimen Kommunikationsschlüssel $z = g(r'^s, r^{s't})$ bilden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Funktion g(.,.) die Multiplikation im endlichen Körper GF(q) ist.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Funktion f(.) eine Einwegfunktion ist.

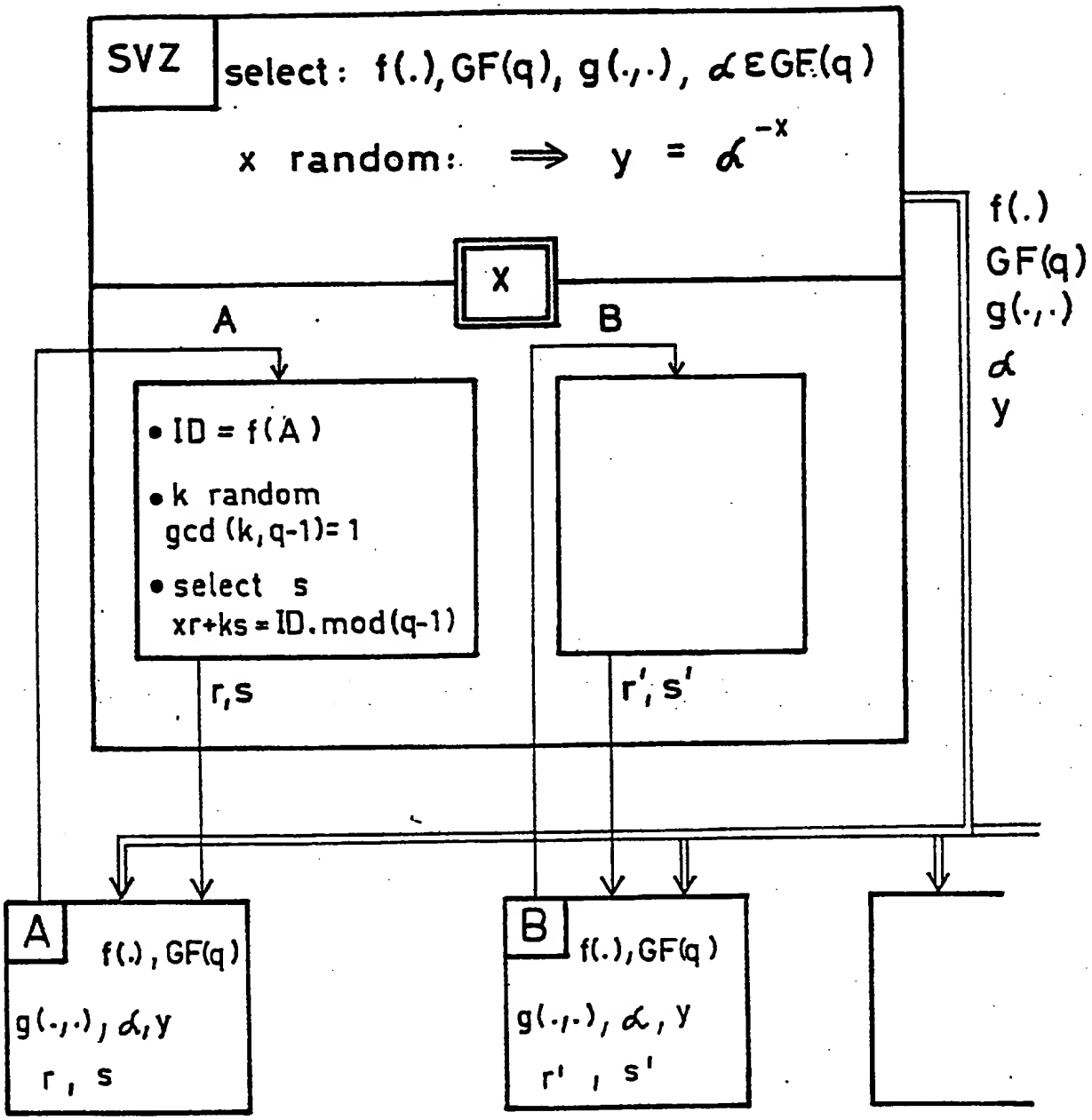

SVZ
select: f(.), GF(q), g(.,.), α ε GF(q)
x random: ⇒ y = α^-x
f(.)
GF(q)
g(.,.)
α
y
X
A
B
• ID = f(A)
• k random
gcd (k, q-1) = 1
• select s
xr+ks = ID. mod(q-1)
r, s
r', s'
A
f(.), GF(q)
g(.,.), α, y
r, s
B
f(.), GF(q)
g(.,.), α, y
r', s'

FIG.1

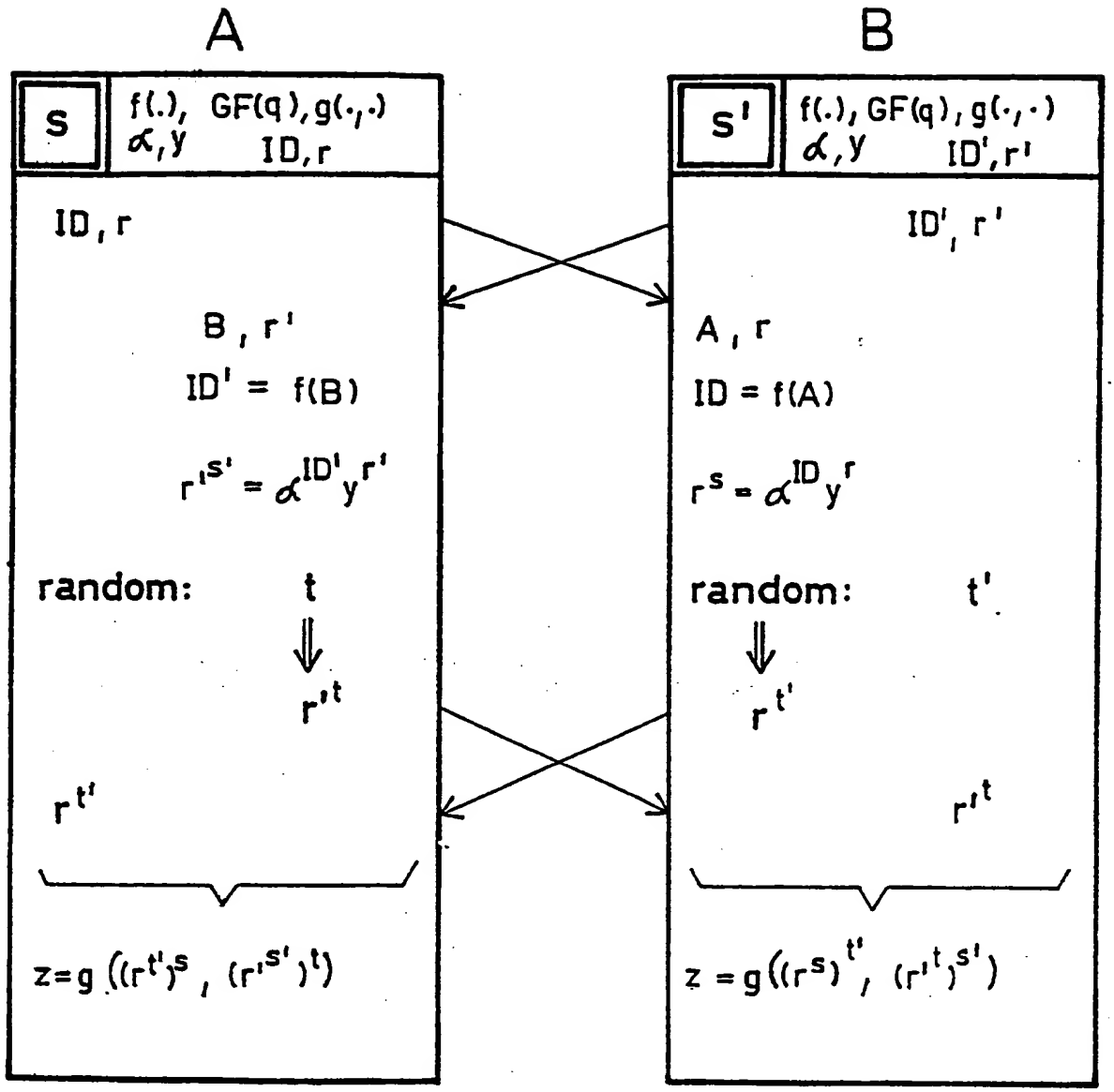

A
B
s
f(.), GF(q), g(·,·)
α, y
ID, r
s'
f(.), GF(q), g(·,·)
α, y
ID', r'
ID, r
ID', r'
B, r'
ID' = f(B)
A, r
ID = f(A)
r'^{s'} = α^{ID'} y r'
r^s = α^{ID} y r
random: t
random: t'
r'^t
r^{t'}
r^{t'}
r'^t
z = g((r^{t'})^s, (r'^{s'})^t)
z = g((r^s)^{t'}, (r'^t)^{s'})

FIG.2

Translation of Swiss Patent Application No. CH 678134 A5

Description

Technical Field

The invention relates to a process for authenticated key-exchange in a network with a key distribution centre and a plurality of subscribers.

The State-of-the Art

Methods for the creation of authenticated secret keys are described, for example, in European patent application EP-A 0 307 627 and in the German AS DE-A 3 915 262.

The first of these two processes transfers the authentication through the public telephone network, and is accordingly not equally appropriate for all uses. The second process utilizes a pre-authenticated list of public subscriber keys and is proposed for automatic operation. However, when establishing the connection, the public subscriber key must be read from the pre-authenticated list. In this situation there are two possibilities: either store the list in each apparatus, which in the case of large networks requires enormous storage space (proportional to the number of subscribers) and requires costly information transfer in the case of network expansion, or the list is

maintained centrally, which requires, for each connection made, two references back to the key distribution centre.

A central list with local extensions is a sensible solution for many applications. However, where the connection is to be autonomously established with restricted storage place and an authentification of the subscriber is individually necessary, the latter process is not very helpful. Examples thereof are networks of POS-terminals, mobile telephone systems, and other wireless networks such as computer networks.

For identification purposes (on PST-terminals inter alia), so-called "zero knowledge proofs" have been suggested by

- Flat and Shamir ("How to Prove Yourself: Practical Solutions to Identification and Signature Problems", Advances in Cryptology – CRYPTO'86, Lecture Notes in Computer Science, Vol. 263,, pp. 186-194, Springer Verlag 1987),
- L.C. Guillou, J.-J. Quisquater ("A Practical Zero Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory, Advances in Cryptology – EUROCRYPT'88, Lecture Notes in Computer Science, Vol. 330, pp. 123-128, Springer Verlag 1988), and by
- T. Beth, ("Efficient Zero Knowledge Identification Scheme for Smart Cards", Advances in Cryptology – EUROCRYPT'88, Lecture Notes in Computer Science, Vol. 330, pp. 77-84 Springer Verlag 1988). In such "zero knowledge proof" systems, each user, in a pre-authentification phase, goes to the code distribution centre, identifies himself, and

receives from the centre the public network key as well as the signature S (ID), belonging to his particular identity ID (for example, AHV-number), which the centre generates with the secret network key.

If A now wishes to identify himself with respect to another user B, he proves in a protocol with B that he knows S(ID) without revealing the signature itself. The signature is thus verified utilizing the public network key.

Description of the Invention

The aim of the invention is to provide a process for authenticated key exchange in a network that has a key distribution centre and numerous subscribers, is flexible in terms of its expansion through new subscribers, has a minimal storage requirement, and avoids the disadvantages of known processes.

In accordance with the invention, the solution is as follows: in a pre-authentication phase,

a) the key distribution centre selects a function f(.) in order to create an identification number, a finite field GF(q), in which the calculating operation is carried out, a function g: GF(q) x GF(q) $\rightarrow$ GF(q), a primitive element $\alpha \varepsilon$ GF(q) and a secret first random number x, from all of which it constructs a public network key $y = \alpha^{-x}$,

b) the key distribution centre assigns to each user an identification number ID = f(A) wherein the key distribution centre selects a secret second random number k which has the characteristics gcd(k,q−1) = 1, constructs from the random number k a public user key $r = \alpha^k$ and a secret user key s with the characteristic xr+ks = ID mod (q−1), and reports to the user both of his two user key,

and that, in a key exchange phase between a first user A and a second user B

c) each of the two users A and B reports to the other his public user code r or r',

d) each of the two users A and B creates the identification number ID' = f(B) or ID = f(A) and from this identification number and the user key r' or r of the other respectively, creates a quantity $r's' = \alpha^{ID'}y^{r'}$ or $r^s = \alpha^{ID}y^r$,

e) each of the two users A and B create a secrete random number t or t', and therewith constructs a code r'^t or $r^{t'}$, which is reported to the other user B or A, and

f) the two users A and B create a common secrete communication key z = $g(r^{t's}, r'^{s't})$.

It is self evident that the finite field GF(q) is so selected that q−1 is a number with at least one large prime factor. All but one of the operations according to the invention are carried out in this field.

In common with the known "zero knowledge proof" process, the invention has the characteristic that it also uses the signature of the identity S(ID) as a secrete

authentication characteristic. In contrast to the known process however, this characteristic is employed for the construction of a secrete, reciprocally authenticated key.

The dependent patent claims cover advantageous embodiments of the invention.

Brief Description of the Drawings

The invention is described in greater detail below, utilizing example embodiments with reference to the drawings, which show:

In Fig. 1 a schematic representation of the pre-authentication phase; and

In Fig. 2 a schematic illustration of the key exchange phase between two users.

The references utilized in the drawings, and their meanings, are found in the list of references (no list attached – transl.).

Ways of Carrying Out the Invention

The key exchange in accordance with the invention takes place in a network suitable for the transfer of digital data, the network having a key distribution centre SVZ and a number of users A, B,...; the network further having two phases, namely a pre-

authentication phase and a key exchange phase. In the pre-authentification phase, each user A, B,..., comes to the key distribution centre SVZ and is assigned an identity according to the El-Gamal-Scheme. In the subsequent key-exchange phase, two users A and B create a common secrete key z in accordance with a modified Diffie-Hellmann process.

Figure 1 shows a schematic representation of the pre-authentification phase. Firstly, the key distribution centre SVZ selects (SELECT) a finite field GF(q), in which q−1 typically has a large prime factor, and a primitive element $\alpha \varepsilon GF(q)$. It then randomly creates (RANDOM), as a secrete network key ("private part") a first number x, from which it creates a public network key ("public part") $y = \alpha^{-x}$. (It is to be understood that the latter and the subsequently described operations take place within the finite field GF(q), when not otherwise explicitly stated.) It further defines a suitable function f(.), which creates a specific identity number from the identity characteristics. Finally, it defines a further suitable function g: $GF(q) \times GF(q) \rightarrow GF(q)$. Preferably this function is the product.

The identity number ID determined by f(.) can, for example, be constructed by scanning the finger (finger print). However other characteristics can also be used. Typically, f(.) is a one way function which is used on the data string and consists of the last name, given name, birth date and possible further characteristics.

The finite field GF(q), the primitive element α and the public network key y as well as the function f(.) are publicly available at the key distribution centre. The secret network key x is stored so as to be inaccessible.

The key distribution centre SVZ has thus concluded the basic common preparations. Now, each user comes to the key distribution centre SVZ, and has his identity designated in accordance with the El-Gamal scheme.

The user A identifies himself (for example, with his passport), whereupon the key distribution centre SVZ, with the help of the function f(.), calculates a specific identity number ID = f(A). Then it randomly creates (RANDOM) a user-specific number k, which has the characteristic gcd(k,q–1) = 1 (gcd – greatest common divisor). From the second random number k it creates a public user key $r = \alpha^k$ and a secrete user key s with the characteristic xr+ks = ID mod (q–1). It reports the two user keys r and s to the user A, who stores the secrete user key s inaccessibly.

Each user wishing to belong to the network must go through the above described pre-authentification phase.

Figure 2 shows a schematic representation of the key exchange phase. It begins with a communication between a first user A and a second user B.

Each of the two users knows the publicly known parameters f(.), g(.,.), GF(q), α, y, as well as his own keys r and s or r' and s'. Typically he will also have his own identity number ID or ID' in storage.

The two users A and B firstly calculate the identity numbers ID' and ID and exchange the public user keys r and r'.

Secondly, each of the two users A and B creates, from the identity number ID', ID and the user key r', r of the other, a quantity $r'^{s'} = \alpha^{ID'}y^{r'}$ or $r^{s} = \alpha^{ID}y^{r}$. In a third step, they each randomly (RANDOM) select a secrete number t, t' and each one calculates therefrom a code r'^{t} or $r^{t'}$. Then these codes r'^{t}, $r^{t'}$ are exchanged. Finally, each of the two users A and B constructs from the known quantity, the common secrete key (session key) $z = g\ (r^{t's}, r'^{s't})$.

The process according to the invention has the following advantages, among others:

1. Aside from one's own identification characteristics, it is sufficient to know a single "public key" to achieve an authenticated key exchange with any other user of the network. The process is characterized as follows using a very small storage capacity.

2. Every pre-authenticated use can achieve an authenticated key exchange with any other pre-authenticated user, without having to refer back to the key

distribution centre (off-line authenticated key exchange). A network driven by this system is as flexible as desired in relation to expansion of the circle of participants.

3. Furthermore, as a result of the key exchange in accordance with the invention, all participants are distinguishable, i.e. no participant can claim to be a different participant.

As to the security of the key exchange in accordance with the invention, the following can be said:

1. If somebody can determine s on the basis of α, y, ID and r, he would be able to break the El-Gamal signature scheme, but this is generally regarded as secure.

2. If somebody can determine $(r^{t'})^s$ from r, r^s and $r^{t'}$, than he could also break the Diffie-Hellmann key exchange algorithm, but this is also generally regarded as secure.

In light of these observations, it appears likely that, with an appropriate selection of q, α, x and k, the knowledge of s and s' is indispensable to the users A and B in the construction of the session key z. The key exchange process in accordance with the invention therefore contains a reciprocal authentification of the users A and B.

The resulting session key z can now be used for a variety of purposes, for example for enciphering, for securing data integrity, or merely for identity control.

The process in accordance with the invention can be realized with means that are known per se. A suitable arrangement for the authenticated key exchange with the aim of enciphering is, for example, described in the above mentioned German AS DE-A 3 9 15 262.

The use possibilities of the described process, relative to the mentioned advantages, are quite broad: mobile telephone, military communication, computer networks and POS-Terminals.

The described key exchange process is a "public key" procedure with a single key which allows an authenticated key creation between any two users. It is drivern off-line, is flexible in connection with expansion by way of new users, and has a small storage requirement. The calculating effort is essentially the same as for the broadly known Diffle-Hellmann process. The somewhat more costly El-Gamal signature is run through by the key distribution centre, only once for each user.

Patent Claims

1. A process for authenticated key exchange in a network with a key distribution centre and a plurality of users A, B, characterized in that, in a pre-authentification phase

a) the key distribution centre selects a function f(.) for creating identity numbers, a finite field GF(q) in which the computation operations are carried out, a function g: GF(q) x GF(q) → GF(q), a primitive element $\alpha \varepsilon$ GF(q) and a secret first random number x, from which it creates a public network key $y = \alpha^{-x}$,

b) the key distribution centre assigns to each user an identity number ID = f(A), wherein the key distribution centre selects a secret second random number k, which has the characteristic gcd(k,q–1) = 1, constructs from the random number k a public user key $r = \alpha^k$ and a secret user key s with the characteristic xr+ks = ID mod (q–1), and reports to the user both of his user keys,

and that in a key exchange phase between a first user A and a second user B

c) each of the two users A, B reports his public user key r, r' to the other,

d) each of the two users A, B creates an identity number ID' = f(B) or ID = f(A), and makes from these identity numbers and the user key r', r of the other, a capacity $r'^{s'} = \alpha^{ID'}y^{r'}$ or $r^s = \alpha^{ID}y^r$,

e) each of the two users A, B creates a secret random number t, t', and creates a code r'^t, $r^{t'}$, which he communicates to the other user B or A, and

f) the two users A and B have a common secret communication key $z = g(r^{t's}, r^{s't})$.

2. A process according to claim 1, characterized in that the function g(.,.) represents multiplication in the finite field GF(q).

3. The process according to claim 1, characterized in that the function f(.) is a one-way function.